THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF TEXAS

JA'QUIL CAPEL, on behalf of himself and all others similarly situated, Plaintiff, v. SYSCO CORPORATION, Defendant.	Case No.: 4:23-cv-02547 DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

The Plaintiff, suing on behalf of himself and others similarly situated (hereinafter "CLASS MEMBERS"), alleges the following against Sysco Corporation (hereinafter "Defendant" or "Sysco") based upon personal knowledge of his own action, investigation by counsel, review of public documents and upon information and belief as to all matters:

INTRODUCTION

1. Plaintiff brings this class action against Sysco for its failure to properly secure and safeguard its current and former employees' sensitive personally identifiable information, including current and former employee's information provided to Sysco for payroll purposes, such as names, Social Security numbers, account numbers, and/or similar information (collectively, "PII").

2. Sysco is an American multination corporation involved in marking and distributing foods products, smallwares, kitchen equipment and tabletop items to restaurants, healthcare and educational facilities, hospitality businesses like hotels and inns, and wholesale to other companies that provide food service.

3. With more than 71,000 employees, Sysco operates 333 distribution facilities worldwide and services around 700,000 customer locations, including restaurants, healthcare, and educational facilities.[1]

4. During the course of their employment with Defendant, Plaintiff and Class Members are required to provide Sysco with their PII. As such Sysco knowingly collects and stores a litany of highly sensitive PII from its current and former employees. In turn, Sysco has a resulting duty to secure, maintain, protect, and safeguard the PII that it collects and stores against unauthorized access and disclosure through reasonable and adequate data security measures.

5. Despite Sysco's duty to safeguard its current and former employees' PII, Plaintiff and Class Members' PII was compromised in a data breach that Defendant became aware on or about March 5, 2023, during which a threat actor

[1] Sergiu Gatlan, *Food distribution giant Sysco warns of data breach after cyberattack*, BleepingComputer (May 9, 2023), https://www.bleepingcomputer.com/news/security/food-distribution-giant-sysco-warns-of-data-breach-after-cyberattack/.

gained access to Sysco's computer systems, thereby compromising the PII stored therein (the "Data Breach").[2]

6. Even though Sysco discovered the Data Breach on or around March 5, 2023, the threat actors initially gained access to Defendant's systems on or around January 14, 2023, meaning the threat actors went undetected in Sysco systems for nearly two months.[3]

7. Based on public information available to data, the information impacted by the Data Breach includes a wide swath of personal information, including current and former employees' information provided to Sysco for payroll purposes, including name, Social Security numbers, account numbers, and/or similar information.[4]

8. As a direct and proximate result of Defendant's failure to implement and follow basic security procedures, Plaintiff's and Class Members' PII has now been exposed to cybercriminals who claim to have exfiltrated said information from Sysco's systems.[5]

9. Plaintiff and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, intrusion of their health privacy, and

[2] *Id.*
[3] *Sysco Data Breach Notification Letter*, https://www.mass.gov/doc/assigned-data-breach-number-29608-sysco-corporation/download, (last visited July 11, 2023).
[4] *Id.*
[5] Gatlan, *supra* note 1.

similar forms of criminal mischief, risk which may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

10. Plaintiff, on behalf of himself and all others similarly situated, alleges claims for negligence, negligence *per se*, and declaratory judgment. Plaintiff seeks damages and injunctive relief, including the adoption reasonably sufficient practices to safeguard PII in Defendant's custody in order to prevent incidents like the Data Breach from reoccurring in the future and for Defendant to provide identity theft protective services to Plaintiff and Class Members for their lifetimes.

PARTIES

11. The Plaintiff, Ja'Quil Capel, is an individual citizen and resident of Mecklenburg County, North Carolina and, at all times relevant herein, was an employee of the Defendant.

12. As a result of the Data Breach, Plaintiff will continue to be at heightened and certainly impending risk for fraud and identity theft, and their attendant damages for years to come.

13. Defendant, Sysco, is a Delaware corporation with a principal place of business in Houston, Texas.

PERSONAL JURISDICTION AND VENUE

14. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member, including Plaintiff, is a citizen of a state different from Defendant to establish minimal diversity.

15. This Court has personal jurisdiction over Defendant because Defendant resides in this district; conducts substantial business in Texas and this District, and collected and/or stored the PII of Plaintiff and Class Members in this District.

16. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant resides in this District, Defendant operates in this District, and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District, including Defendant collecting and/or storing the PII of Plaintiff and Class Members.

STATEMENT OF FACTS COMMON TO ALL COUNTS

17. Plaintiff hereby incorporates by reference and repleads all prior paragraphs of this Complaint.

18. According to Sysco, it "is the global leader in selling, marketing and distributing food and non-food products to restaurants, healthcare and educational facilities, lodging establishments and other customers around the world."[6]

19. Sysco employs more than 71,000 people and in the course of that employment Sysco collects and stores employee PII, which includes, *inter alia* information provided to Sysco for payroll purposes, including names, Social Security numbers, account numbers, and/or similar information.

20. Indeed, as a condition of their employment, Plaintiff and Class Members directly or indirectly entrusted Sysco with their sensitive PII and therefore reasonably expected that Defendant would safeguard their highly sensitive information.

21. By obtaining, collecting, and storing Plaintiff's and Class Members' PII, Sysco, assumed equitable and legal duties to safeguard Plaintiff's and Class Members' highly sensitive information, to only use this information for business purposes, and to only make authorized disclosures.

22. Despite these duties, Sysco failed to implement reasonable data security measures to protect Plaintiff's and Class Members' PII and ultimately allowed threat

[6] *The Sysco* Story, Sysco, https://www.sysco.com/About/Company-Profile/The-Sysco-Story.html, (last visited July 11, 2023).

actors to breach its computer systems and exfiltrate Plaintiff's and Class Members' PII.

23. On or about May 5, 2023, Sysco revealed, through notifications to employees, such as the Plaintiff, that a data breach within its system had harmed approximately126,000 current and former employees across the country. Specifically, and as a result of this data breach, unauthorized parties gained access to current and former employees' personal and private information, which includes names, address, Social Security numbers, financial account numbers, and other personal information.

24. Sysco learned of the data breach on or about March 5, 2023, but did not announce such breach until May 5, 2023 as indicated below.

25. Such data breach occurred as a result of Sysco's failure to appropriately implement and/or maintain sufficient and adequate security measures and to otherwise take reasonable care of said personal and private information. Specifically, Sysco willfully ignored warnings and known weaknesses within its security system which allowed said system to be accessed by unauthorized third parties, subjecting approximately 126,000 current and former employees, including Plaintiff, to substantial fraud, credit harm and identity theft.

26. Class members, and this Plaintiff particularly, have incurred or will incur significant out-of-pocket expenses in order to obtain credit reports, credit

monitoring, credit freezes and other various measures to protect and repair their financial security as a direct impact of said data breach.

27. In relevant part, Sysco's privacy policy statement promises to consumers the following:

> Sysco takes the security of your personal data seriously. We maintain technical and organizational measures to protect your personal data and have established policies and processes in place to manage any suspected personal data breach. We limit access to your personal data to those employees, contractors, service providers or other parties to whom we disclose, or make available your personal data to those who have a business need to know. We also practice data minimization and strive to collect no more personal data from you than is required by the purpose for which we collect it.[7]

The Value of Private Information and Effects of Unauthorized Disclosures

28. Sysco was well aware that the PII it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

29. Sysco also knew that a breach of its computer systems, and exposure of the PII stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised.

30. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at business such as Equifax, Facebook, Yahoo, Marriott, Anthem, and many others.

[7] https://www.sysco.com/Privacy-Notice.html (last accessed July 11, 2023).

31. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers can easily sell stolen data as there has been "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[8]

32. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud.[9]

33. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2021, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[10]

34. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[11]

---

[8] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

[9] https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft

[10] *Data Breach Report: 2021 Year End*, Risk Based Security (Feb. 4, 2022), https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/.

[11] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited July 11, 2023).

35. The ramifications of Sysco's failure to keep Plaintiff and Class Members' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[12]

36. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

[12] U.S. Gov't Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited July 11, 2023).

37. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's employees especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

38. **Social Security Numbers**—Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique social security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

39. Indeed, even the Social Security Administration warns that the process of replacing a Social Security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.

> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[13]

40. Social security numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often social security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes social security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

41. **Financial Account Information**—Stolen financial account information can have an equally devasting impact on consumers. Cybercriminals can deplete and wipe out a person's life savings or take out a loan or mortgage against someone's home with the click of a button.

42. Based on the value of its current and former employees' PII to cybercriminals, Sysco knew or should have known, the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its data security systems

[13] *Identify Theft and Your Social Security Numbers*, Social Security Admin. (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

were breached. Sysco failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

Transportation Companies are Particularly Vulnerable to Data Breaches

43. Sysco also knew or should have known that transportation companies, such as itself, have become prime targets for cybercriminals in recent years.

44. Transportation and logistics is one of the most important industries in the world. "However, because it is so heavily dependent on technology, it is also one of the most vulnerable to cybercrime. Cyber-attacks have been targeting the transportation and logistics industries in many ways and can impact daily operations for extended periods. Not only is service disrupted, but the exposure of highly sensitive data is also a huge risk when it comes to this sector."[14]

45. According to Cybertalk.org, between 2020 and June 2021, the transportation sector witnessed a 186 percent increase in weekly ransomware attacks.[15] While the number of ransomware attacks has been increasing across all industries, transportation companies have been targeted at a higher rate in part "[b]ecause transportation companies have not historically deployed large security

[14] April Miller, *Cybersecurity Attacks & the Transportation Industry*, Cyber Management Alliance (Oct. 19, 2021), https://www.cm-alliance.com/cybersecurity-blog/cybersecurity-attacks-the-transportation-industry.

[15] *Ransomware attacks on the transportation industry, 2021*, CyberTalk.org (July 28, 2021), https://www.cybertalk.org/2021/07/28/ransomware-attacks-on-the-transportation-industry-2021/.

teams to protect their digital assets" and they "are more acutely affected by the global cybersecurity skills gap than other businesses."[16]

46. Indeed, there has been no shortage of notable cyber-attacks in the transportation industry in recent years. In 2020, the giant shipping company Matson was subjected to a ransomware attack during which the attackers exfiltrated data and then encrypted it, threating to release the stolen data on the dark web if Matson did not pay the ransom demand.[17]

47. Similarly, in March 2021, ATC Transportation fell victim to a ransomware attack during which cybercriminals accessed the company's servers and installed malware.[18] The cybercriminals then encrypted ATC Transportation's data, holding it for ransom, compromising the personal information of current and former employees, and job applicants.[19]

48. As a transportation company, Sysco knew, or should have known, the importance of safeguarding the PII its current and former employees entrusted to it and the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Defendant's current and

[16] Steven Bowcut, *Cybersecurity in the transportation industry*, Cybersecurity Guide (last updated Nov. 10, 2022), https://cybersecurityguide.org/industries/transportation/.
[17] *Id.*
[18] *Id.*
[19] *Id.*

former employees as a result of a Data Breach. Sysco failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

Sysco Breached its Duty to Protect Current and Former Employees' PII.

49. On or about March 5, 2023, Sysco became aware of a cybersecurity event that was believed to have begun on January 14, 2023.[20] As such, a threat actor went undetected in Sysco's computer systems for nearly two months.

50. After becoming aware of the Data Breach, Sysco opened an investigation and engaged a cyber security firm and other experts.[21]

51. According to Sysco, during the Data Breach the threat actor gained access to its systems without authorization and claimed to have acquired certain data related to the personal information of current and former Sysco employees. [22]

52. The current and former employee information compromised during the Data Breach includes, at the very least, personal information provided to Sysco for payroll purposes, including names, Social Security numbers, account numbers, and/or similar information.[23]

53. While Sysco claims it has not yet validated the threat actor's claims, Defendant reported report to the U.S. Securities and Exchange Commission that its

[20] *Sysco Data Breach Notification Letter*, *supra* note 3.
[21] *Id.*
[22] *Id.*
[23] *Id.*

investigation determined that the threat actor "extracted certain company data, including data relating to operation of the business, customers, employees and personal data."[24]

54. On or around May 5, 2023, nearly four months after the Data Breach began, Sysco reported the Data Breach to the Office of the Main Attorney General, indicating the Data Breach compromised approximately the PII of approximately 126,000 current and former employees.[25]

55. On or around the same time, Plaintiff received a notification, informing him that his PII had been compromised during the Data Breach.

56. Upon information and belief, Class Members received similar notices informing them that their PII was compromised during the Data Breach.

57. The details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

---

[24] *Sysco Corp. Form 10-Q 2023* (May 2, 2023), https://otp.tools.investis.com/clients/us/sysco1/SEC/sec-outline.aspx?FilingId=16611993&Cik=0000096021&PaperOnly=0&HasOriginal=1.

[25] *Data Breach Notifications*, Office of the Main Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/28ded7f7-4f72-4a32-b531-1ba31469d1aa.shtml (last visited July 11, 2023).

58. The Data Breach occurred as a direct result of Sysco's failure to implement and follow basic security procedures in order to protect its current and former employees' PII.

59. Upon information and belief, Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing the exposure of PII for Plaintiff and Class Members.

FTC Guidelines Prohibit Sysco from Engaging in Unfair or Deceptive Trade Acts or Practices

60. Sysco is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

61. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[26]

[26] *Start with Security – A Guide for Business*, United States Federal Trade Comm'n (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

62. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[27]

63. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[28]

64. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

[27] *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformationpdf.
[28] *Id.*

65. Sysco failed to properly implement basic data security practices. Sysco's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PII constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

66. Sysco was at all times fully aware of its obligations to protect the PII of consumers because of its position as an employer, which gave it direct access to reams of PII. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Damages to Plaintiff and Class Members

67. The ramifications of Sysco's failure to keep PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

68. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct. Further, the value of Plaintiff and Class members' PII has been diminished by its exposure in the Data Breach.

69. Plaintiff and Class members are at substantial increased risk of suffering identity theft and fraud or misuse of their PII as a result of the Data Breach.

From a recent study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[29]

70. Further, Plaintiff and Class members have incurred and will incur out of pocket costs for protective measures, such as identity theft protection, credit monitoring, credit report fees, credit freeze fees, and similar costs related to the Data Breach.

71. Besides the monetary damage sustained in the event of identity theft, consumers may have to spend hours trying to resolve identity theft issues. For example, the FTC estimates that it takes consumers an average of 200 hours of work over approximately six months to recover from identity theft.[30]

72. Plaintiff and Class members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its employees' and consumers' PII.

---

[29] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KnowBe4, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last visited July 11, 2023).

[30] Kathryn Parkman, *How to Report identity Theft*, ConsumerAffairs (Feb. 17, 2022), https://www.consumeraffairs.com/finance/how-to-report-identity-theft.html.

73. Plaintiff and Class members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private information to strangers.

74. As a result of Sysco's failure to prevent the Data Breach, Plaintiff and Class members have suffered and will continue to suffer injuries, including out of pocket expenses; loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the Data Breach; theft of their valuable PII; the imminent and certainly impeding injury flowing from fraud and identity theft posed by their PII being disclosed to unauthorized recipients and cybercriminals; damages to and diminution in value of their PII; and continued risk to Plaintiff's and the Class members' PII, which remains in the possession of Defendant and which is subject to further breaches so long as Sysco fails to undertake appropriate and adequate measures to protect the PII that was entrusted to it.

CLASS ACTION ALLEGATIONS

75. Plaintiff hereby incorporates by reference and repleads all prior paragraphs of this Complaint.

76. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 on behalf of a Class consisting of all citizens in the United States who had their personal and private identifying information exposed to unauthorized third parties

as a result of the aforementioned data breach discovered on or about March 5, 2023 (hereinafter "the Class").

77. This Plaintiff is a member of the Class which they seek to represent.

78. The Class consists of thousands of individuals within the United States and therefore is so numerous that joinder is impracticable. The exact numbers and identities of the individual class members are identifiable through Defendant's records, including but not limited to those files exposed in the Data Breach.

79. The claims of this Plaintiff are typical of the claims of the Class because they and all members of the Class have or likely will incur significant out-of-pocket expenses in order to obtain credit reports, credit monitoring, credit freezes and other various measures to protect and repair their financial security as a direct impact of said data breach. Additionally, Plaintiff and all members of the Class have been exposed to the substantial risk of fraud, credit harm and/or identity theft.

80. There are numerous questions of law and fact common to the Class which predominate over any questions affecting only individual class members, including, but not limited to, the following:

a. Whether Sysco acted negligently and with due diligence with regards to protecting personal and private Class Member information from risk of such data breach;

b. Whether Sysco acted willfully and with wanton abandon in the face of known risks of such a data breach or risks of such a data breach that, with the application of reasonable care and due diligence, should have been known, in order to maximize profits at the expense of Class Members' financial safety;

c. Whether Sysco acted negligently and in an untimely manner upon knowledge of the data breach on March 5, 2023;

d. Whether the Plaintiff and Class Members are entitled to equitable relief as a result of said data breach; and

e. Whether the Plaintiff and Class Members are entitled to recover money damages as a result of said data breach.

81. All common questions are able to be resolved through the same factual occurrences as specifically and/or generally alleged herein.

82. Plaintiff will fairly and adequately represent and protect the interests of the Class and have no claims antagonistic to those of the Class. Plaintiff has retained competent and experienced counsel in complex class actions, mass tort and product liability litigation and counsel is committed to the vigorous prosecution of Plaintiff's and the Class Members' claims.

83. Prosecution of separate actions by the Plaintiff and individual members of the Class against the Defendant will create a risk of inconsistent or varying adjudications on the common issues of law and fact related to this action.

84. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy because:

a. Given the number of Class Members involved, a class action is the only "fair and efficient" means to adjudicate the controversy;

b. Multiple lawsuits will be costly, inefficient and duplicative;

c. Relatively few Class Members will have been damaged to a degree that would induce them to initiate litigation solely on their own behalf;

d. The public interest in protecting the rights of such Class members favors disposition of the controversy in the class action form;

e. The class members can be identified from Sysco's files; and

f. There are no manageability problems that would create a situation that would be less fair and efficient than other options.

85. In addition, the expense and burden of litigation would substantially impair the ability of Class members to pursue individual cases to protect their rights.

86. Class certification under Fed. R. Civ. P. 23 (b) (1) is appropriate because adjudications with respect to individual members of the Class would be as a practical matter dispositive of interests of the other members not parties to these adjudications.

87. Class certification under Fed. R. Civ. P. 23(b)(2) is appropriate because Sysco has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole.

88. Class certification under Fed. R. Civ. P. 23(b)(3) is appropriate because the common issues of fact and law alleged herein are common to the Class and predominate over any questions affecting only individual members, thereby rendering the class action superior to all available methods for the fair and efficient adjudication of this controversy.

COUNT 1
Negligence
(On Behalf of Plaintiff and the Class)

89. Plaintiff hereby incorporates by reference and repleads all prior paragraphs of this Complaint.

90. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

91. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

92. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiff and the Class in Defendant's possession was adequately secured and protected.

93. Defendant also had a duty to exercise appropriate clearinghouse practices to remove from an Internet-accessible environment the PII it was no longer required to retain pursuant to regulations and had no reasonable need to maintain in an Internet-accessible environment.

94. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and the Class.

95. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Defendant acquired Plaintiff's and the Class's confidential PII in the course of its business practices.

96. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

97. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of

Defendant's inadequate security practices.

98. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

99. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

100. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

101. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

102. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the

Class to (i) take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties and (ii) prepare for the sharing and detrimental use of their sensitive information.

103. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Class.

104. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

105. Specifically, Sysco breached one or more of the following duties to Plaintiff and the Class Members:

a. The duty to adequately protect the privacy and confidentiality of Plaintiff and the Class Members personal and private information;

b. The duty to implement, maintain and timely update security measures to prevent a foreseeable data breach like or similar to the subject data breach;

c. The duty to implement, maintain and timely update security measures to detect a foreseeable data breach like or similar to the subject data breach;

d. The duty to disclose in as timely and appropriate a manner as feasible, that their data security practices were inadequate and/or incomplete and would thus potentially expose Plaintiff and Class Members to unauthorized third-party access to personal and private information like or similar to the information accessed in the subject data breach;

106. As a result of said negligence, Plaintiff and the Class Members were damaged through exposure of their personal and private information and have suffered injuries to include:

a. Theft of their PII;

b. Costs associated with requested credit freezes;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of the PII;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data

Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

g. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of cyber-criminals;

h. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members data against theft and not allow access and misuse of their data by others; and

i. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

107. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and

other economic and non-economic losses.

108. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

109. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

Count 2
Negligence Per Se
(On Behalf of Plaintiff and the Class)

110. Plaintiff restates and realleges all preceding factual allegations above as if fully set forth herein.

111. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by institutions such as Defendant or failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

112. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of

PII it obtained and stored and the foreseeable consequences of a data breach within the transportation sector.

113. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

114. Moreover, the harm that has occurred is the type of harm that the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

115. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

116. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

Count 3
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

117. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

118. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

119. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and whether Sysco is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII. Plaintiff alleges that Sysco's data security measures remain inadequate, Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his PII and remains at imminent risk that further compromises of his PII will occur in the future.

120. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Sysco owes a legal duty to secure employees' PII and to timely notify employees of a data breach under the common law, Section 5 of the FTC Act, and various state statutes; and

b. Sysco continues to breach this legal duty by failing to employ reasonable measures to secure employees' PII.

121. This Court also should issue corresponding prospective injunctive relief requiring Sysco to employ adequate security protocols consistent with law and industry standards to protect employees' PII.

122. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Sysco. The risk of another such breach is real, immediate, and substantial. If another breach at Sysco occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and he will be forced to bring multiple lawsuits to rectify the same conduct.

123. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Sysco if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Sysco of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Sysco has a pre-existing legal obligation to employ such measures.

124. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach at Sysco, thus eliminating the additional injuries that would result to Plaintiff and employees whose confidential information would be further compromised.

NOW THEREFORE, the Plaintiff on behalf of himself and all members of the Class, request a jury trial on all claims so triable and pray the following relief:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

b. An award in the amount of fair compensation for compensatory, consequential, incidental, statutory damages and restitution as provided by law and determined at trial;

b. Injunctive relief requiring Sysco to promptly and adequately update and/or strengthen its security measures to appropriately protect Class Members' personal and private information to comply with any applicable federal and local laws and to adhere to the best practices of the industry;

c. Attorneys' fees as permitted by state and local statute.

d. Pre- and post-judgment interest in the statutory amount.

e. All costs of this action to be recovered as permitted by law.

f. Any other further relief as the Court deems appropriate.

Date: July 11, 2023

Respectfully Submitted,

/s/*William B. Federman*
William B. Federman,

S.D. Tex. Bar No. 21540
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
P: (405) 235-1560 F: (405) 239-2112
wbf@federmanlaw.com

Gary F. Lynch*
LYNCH CARPENTER LLP
1133 Penn Ave., 5th Floor
Pittsburgh PA, 15222
P: (412) 322-9243
gary@lcllp.com

Jeremy McDonald*
Chandler & McDonald, PLLC
101 N. McDowell St., Suite 210
Charlotte, North Carolina 28204
Telephone: (704) 376-6552
Fax: (704) 372-2003
Jmcdonald@charlottelawoffice.com

Theodore H. Huge*
Harris & Huge, LLC
180 Spring Street
Charleston, SC 29403
Telephone: (843) 805-8031
Fax: (843) 636-3375
ted@harrisandhuge.com

**pro hac vice forthcoming*

Attorneys for Plaintiff and
the Proposed Class